



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------|------------------|
| 10/804,487 | 03/18/2004 | Shlomo Ovadia | 42P18636X | 7601 |
| 7590 08/11/2008 | | | | |
| R. Alan Burnett BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP Seventh Floor 12400 Wilshire Boulevard Los Angeles, CA 90025 | | | | |
| EXAMINER TESLOVICH, TAMARA | | | | |
| ART UNIT PAPER NUMBER | | | | |
| 2137 | | | | |
| MAIL DATE DELIVERY MODE | | | | |
| 08/11/2008 PAPER | | | | |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/804,487

Applicant(s)

OVADIA, SHLOMO

Examiner

Tamara Teslovich

Art Unit

2137

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 January 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-15 and 44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15 and 44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-8508)
Paper No(s)/Mail Date 10.12.07
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

This Office Action is in response to Applicant's Remarks and Amendments filed January 18, 2008.

Claim 16 is cancelled.

Claims 1, 6, 19, and 28-33 are amended.

Claims 1-15 and 17-44 are pending and herein considered.

Response to Arguments

Applicant's arguments filed January 18, 2008 have been fully considered but they are not persuasive.

In regards to Applicant's remarks concerning the references' alleged failure to teach or suggest distributing encryption keys within control bursts of an optical-switched network used to reserve network resources and form virtual lightpaths between edge nodes as recited in claim 1, the Examiner respectfully disagrees. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). The Examiner's rejection of claim 1 was based upon the combination of the Microsoft TechNet article and the Rouskas paper. The Rouskas paper disclosed the use of optical switched networks including the use of VPNs therein, or "simply a set of client edge nodes that need to be interconnected by lightpaths with certain protection

requirements". It was based in part on this description that the Microsoft article was brought in to provide additional details regarding the use of secure keys within VPNs, regardless of the system. It is based upon this combination that the Examiner maintains her rejection of the claims for the reasons given above and in view of the references in their entirety. Furthermore, the use of optical bursts and communication signals within an optical-switched network may be found in the Rouskas, particularly pages 301-302.

In regards to Applicant's remaining remarks concerning the remaining claims and their dependence upon allowable claims, the Examiner respectfully maintains the rejection of all independent and dependent claims based upon those remarks given above in view of the previous rejection and the references in their entirety.

Information Disclosure Statement

The information disclosure statement received 21 July 2005 has not been considered. The information disclosure statement includes well over 100 documents, encompassing thousands of pages, and there is no explanation of relevance or any other statement to suggest which of the references or which portions of the references are considered to be pertinent to the present application. Therefore, a requirement for information under 37 CFR 1.105 is set forth and attached to this Office action, requiring Applicant to state which of the cited references are considered to be of particular relevance to the present application. The information disclosure statement has been placed in the application file, but the information referred to therein has not been considered.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-15 and 17-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the encrypted data that are sent." There is insufficient antecedent basis for this limitation in the claim. The Examiner is under the impression that Applicant intended for "the data" of line 12 to read "the encrypted data."

Claims 5-9, 13-15, and 17-18 recite the phrases "the edge node," "the other edge node" and variations thereof. There is insufficient antecedent basis for these phrases in the claim as a result of Applicant's amendments to dependent claim 1. Applicant is required to amend all claims depending on claim 1 in such a way that they may conform to the language and structure utilized by the independent claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 5-9, 19, 26 and 28, are rejected under 35 U.S.C. 103(a) as being unpatentable over Rouskas I. ("Optical Network Engineering, 2003) in view of Microsoft TechNet ("Virtual Private Networking: an Overview", 09/04/2001).

Regarding **claims 1, 5, 19 and 28**, Rouskas discloses an Optical Network using a virtual private network (VPN) to provide secure communication between the destination edge node and the source edge node (page 315, lines 33-37); transmitting control bursts containing information to reserve network resources to form a virtual lightpath between the destination and source edge nodes (see figure 10.1 and page 301; see page 302); sending the data along a virtual lightpath between the source and destination nodes (page 299-300, para. 2, lines 8-12 and lines 17-18), the virtual lightpath spanning at least one lightpath segment (page 299, para 2, lines 12-13); during a schedule timeslot (page 305, lines 6-12; a control unit for sending signals (see figure 10.1 and page 301; see page 302).

However Rouskas does not discloses generating, at least one edge node in the OS network, security keys including an encryption key and a decryption key; distributing, for said destination edge node, the encryption key to the source edge node in the OS network; encrypting, at a source edge node, data to be sent from the source edge node to a destination edge node, said data encrypted with an encryption key distributed by the destination node and received by the source node; and decrypting, at the destination edge node, the encrypted data that are sent, said encrypted data being decrypted with the decryption key generated by the destination node.

Microsoft TechNet discloses a VPN uses an asymmetric key encryption (page 14, lines 57-58; page 15, lines 1); distributing for said destination edge node, the encryption key to a source edge node. Distributing a key to nodes is an intrinsic property of an asymmetric key encryption (page 15, lines 1); encrypting at a source node data to be sent from the source node to a destination node, it is also known to encrypt data with the public key and decrypt data with a private key in asymmetric encryption (page 15, lines 16-18); decrypting at the destination edge node data that are sent (page 15, line 18).

Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Rouskas to include the use of an asymmetric key encryption in order to have a pair for encrypting and decrypting of information between two nodes, such that information may be protected during transmission.

Regarding **claim 6**, Microsoft TechNet discloses a public key encryption, distributed with a certificate (public key certificate) to the receiver (see page 15, lines 22-36).

Regarding **claim 7**, Microsoft TechNet discloses signing a digital certificate and sending it to the receiving party (page 15, lines 28-32).

Regarding **claim 8**, Microsoft TechNet discloses generating security data including public key at the generation edge node (page 15, lines 16-20); sending the

Art Unit: 2136

security data to a certificate authority (page 15-, lines 23-24); the certification authority to issue an authenticated digital certificate containing the public key page 15, lines 25-26); and receiving the authenticated digital certificate at the receiving node (page 15, lines 18).

Regarding **claim 9**, Microsoft TechNet discloses generating a respective set of security data at each node; and sending the respective set of security data from the nodes to the certificate authority (page 15, lines 14-20).

Regarding claim **26**, Microsoft TechNet discloses usage rules for the certificate and expiration date to allow information to be decrypted or not decrypted (page 15, lines 25-26).

Claims 10-15, 17-18, 23-25, 27 and 29-33, are rejected under 35 U.S.C. 103(a) as being unpatentable over Rouskas I. ("Optical Network Engineering, 2003) in view of Microsoft TechNet ("Virtual Private Networking: an Overview", 09/04/2001) futher in view of (Proudlar (US 2003/0110372 A1).

Regarding **claims 10, 23-25 and 29-31**, Rouskas and Microsoft TechNet disclose all the limitations of claim 10, except for employing a trusted platform module (TPM) to generate an asymmetric key pair.

Proudlar discloses generating an asymmetric key pair (para. 0005, lines 11-15); and a symmetric key (para. 0005, lines 2-3).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Rouskas to include the use of a trusted platform module (TPM) in order to provide a secure facility to generate cryptographic keys as well as to limit the use of the keys.

Regarding **claim 11**, Proudler discloses employing the TPM to securely store the decryption key, against unauthorized party (para. 0005, lines 13-15; para. 0010, lines 15-16).

Regarding **claims 12 and 33**, Proudler discloses a TPM generating a security key (para. 0005, lines 13-16); encrypting one of a decryption key or digital certificate containing a decryption key using the security key (para. 0005, lines 16-27); measuring an integrity metric corresponding to a platform configuration (para. 0010, lines 5-14); storing the integrity metric in a platform configuration register (PCR) sealing the security key against the TPM using a TPM_Seal command referencing the PCR (para. 0010, lines 40-50).

Regarding **claim 13**, Proudler discloses employing a TPM accessible to a node that receives an encryption key to securely store the encryption key from unauthorized parties (para. 0005, lines 13-15).

Regarding **claims 14-15**, Proudler discloses a distribution system to distribute security keys using out-of-band channels (para 0005, lines 5-9).

Regarding **claims 17-18, 27 and 32**, Rouskas discloses sending information to each node identifying at least one of an encryption algorithm and decryption algorithm to be employed to encrypt and/or decrypt the data via security keys (page 315, lines 34-44).

Claims 2-4 and 20-22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Rouskas I. ("Optical Network Engineering, 2003) in view of Microsoft TechNet ("Virtual Private Networking: an Overview", 09/04/2001) further in view of Sahara et al. ("Demonstration of Optical Burst Data Switching Using Photonic MPLS Routers Operated by GMPLS signaling~ Vol. 1, 2003).

Regarding **claims 2 and 20**, Rouskas and Microsoft TechNet discloses all the limitation of claim 2, except for the optical switch network comprises an optical burst-switched (OBS) network.

Sahara discloses an optical burst network (page 220, figure 1; col. 3, lines 25).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Rouskas and Microsoft TechNet to include the use of optical burst switched network in order to better improve the utilization of wavelength by rapid setup switching and teardown of the wavelength/lightpath for incoming bursts.

Regarding **claims 3 and 21**, Sahara discloses a photonic burst switched network (page 220, col. 3, lines 13-18).

Regarding **claims 4 and 22**, Sahara discloses a wavelength-division multiplexed (page 1, col. 1, lines 16-19).

Claims 34-44, are rejected under 35 U.S.C. 103(a) as being unpatentable over Rouskas I. ("Optical Network Engineering, 2003) in view of Microsoft TechNet ("Virtual Private Networking: an Overview", 0910412001) in view of Sahara et al. ("Demonstration of Optical Burst Data Switching Using Photonic MPLS Routers Operated by GMPLS signaling" Vol. 1, 2003) Further in view of (Prouder (US 2003/0110372 A1)

Regarding **claim 34, 39, 40, and 43** Rouskas discloses an Optical Network using a virtual private network (VPN) to provide secure communication for the edge nodes (page 315, lines 33-37); sending the data along a virtual lightpath between the source and destination nodes (page 299-300, para. 2, lines 8-12 and lines 17-18), the virtual lightpath spanning at least one lightpath segment (page 299, para 2, lines 12-13); during a schedule timeslot (page 305, lines 6-12; a control unit for sending signals (see figure 10.1 and page 301; see page 302); a processor is an intrinsic property of the claimed invention as encryption and decryption cannot take place without a processor. The limitation of an interface is an intrinsic property of the claimed invention, as communication cannot take place without if no interface exists between the nodes.

However Rouskas does not discloses generating, at least one edge node in the OS network, security keys including an encryption key and a decryption key; distributing, for said at least one edge node, the encryption key to at least one other edge nodes in the OS network; encrypting, at a source edge node, data to be sent

from the source edge node to a destination edge node, said data encrypted with an encryption key distributed by the destination node and received by the source node; and decrypting, at the destination edge node, the encrypted data that are sent, said encrypted data being decrypted with the decryption key generated by the destination node.

Microsoft TechNet discloses a VPN uses an asymmetric key encryption (page 14, lines 57-58; page 15, lines 1); distributing a key to at least one node, the encryption key to at least one other nodes. Distributing the a key to nodes is an intrinsic property of an asymmetric key encryption (page 15, lines 1); encrypting at a source node data to be sent from the source node to a destination node, it is also known to encrypt data with the public key and decrypt data with a private key in asymmetric encryption (page 15, lines 16-18); decrypting at the destination edge node data that are sent (page 15, line 18).

Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Rouskas to include the use of an asymmetric key encryption in order to have a pair for encrypting and decrypting of information between two nodes, such that information may be protected during transmission.

Rouskas does not disclose data to be sent to the destination node operatively linked in communication to the system via photonic burst-switched.

Sahara discloses a photonic burst switched for sending data to a node (see figure 1; page 220, col. 3, lines 13-18).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Rouskas and Microsoft TechNet to include the use of photonic burst switched in order to switch individual wavelengths of light onto separate paths for specific routing information.

Rouskas does disclose a trusted platform module (TPM) commanding a symmetric session key or an asymmetric key session key pair for encryption and decryption.

Proudlar discloses a TPM commanding a symmetric session key and an asymmetric session key pair for encryption and decryption of information (para. 0004, line 1-14; para. 0005, lines 5-16).

Therefore it would have been obvious to one of Ordinary skill in the art at the time of the invention to modify Rouskas, Microsoft TechNet and Sahara to include the use of a trusted platform module in order to provide a facility for secure generation of cryptographic keys, such that one may have the ability to limit the use of keys to either signing/verification or encryption/decryption.

Regarding **claims 35-36**, the limitation of "said at least one processor include a network processor and egress, ingress network processors are intrinsic property of the claimed invention as the claimed invention is taking place in a network using network switches/routers.

Regarding **claim 37**, Proudler discloses a TPM, which is a chip (hardware) (see figure 1 of the drawing).

Regarding **claim 38 and 41**, Proudler discloses wherein the *encryption/decryption* component embodied as a software, module comprising a plurality of instructions to effectuate *encryption/decryption* operation when executed on a processor (para. 0010, lines 33-40).

Regarding **claim 42 and 44**, Microsoft TechNet discloses a time-bound decryption key to prevent decryption upon expiration of a date (time) (page 15, lines 25-28).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

Art Unit: 2136

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571)272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2137

Art Unit: 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136